RC24559 (W0805-086) May 13, 2008
Computer Science

IBM Research Report

Inter-Domain Routing for Mobile Ad Hoc Networks

Chi-Kin Chau, Jon Crowcroft
Computer Laboratory
University of Cambridge
UK

Kang-Won Lee, Starsky H. Y. Wong
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
USA

Inter-Domain Routing for Mobile Ad Hoc Networks

Chi-Kin Chau, Jon Crowcroft
Computer Laboratory
University of Cambridge, UK
chi-kin.chau,jon.crowcroft@cl.cam.ac.uk

Kang-Won Lee, Starsky H.Y. Wong
IBM T.J. Watson Research Center
Hawthorne, NY, USA
kangwon,hwong@us.ibm.com

ABSTRACT

Inter-domain routing is an important component to allow interoperation among heterogeneous network domains operated by different organizations. Although inter-domain routing has been well supported in the Internet, there has been relatively little support to the Mobile Ad Hoc Networks (MANETs) space. In MANETs, the inter-domain routing problem is challenged by: (1) dynamic network topology due to mobility, and (2) diverse intra-domain ad hoc routing protocols. In this paper, we discuss how to enable inter-domain routing among MANETs, and to handle the dynamic nature of MANETs. We first present the design challenges for inter-domain routing in MANETs, and then propose a framework for inter-domain routing in MANETs.

Categories and Subjects: C.2.1 [Computer-Communication Networks]:network protocols, internetworking

General Terms: Design, Evaluation

Keywords: Mobile ad hoc networks, Inter-domain routing, Policy-based Routing

1. INTRODUCTION

Mobile ad hoc networks (MANETs) can enable effective communications in dynamic operation environments including a coalition military operation, emergency operation for disaster recovery, and on-the-fly team formation for a common mission, such as search and rescue. In these situations, multiple groups and organizations need to come together, communicate, and collaborate to achieve a common goal. For example, in a disaster recovery scenario, the local police force may need to coordinate with fire fighters, military forces, and medical crews by sharing information and communicating with each other regardless of the particular networking technologies that each group uses.

Another practical usage of MANETs in the near future is in the context of vehicular area networks (VANETs). In this scenario, groups of cars on the road will instantly form a communication network for sharing traffic information, preventing accidents, and data sharing. However, it is unlikely all cars will support the same network technologies, not to mention belong to the same network. The VANET for a particular car will be based on various factors such as auto manufacturer (who may employ a common network service for its own cars), service plans (people may subscribe to a network service plan of their own choosing), and other personal/business imperatives (employees of a company may be on the same network service). However, a single VANET may not be connected all the time and may only reach others via other VANETs. Such application scenarios call for development of a technology to enable end-to-end communications over heterogeneous MANETs governed by distinct administrative domains.

Facilitating interoperation among multiple MANETs presents a significant challenge at multiple levels, from physical to application layers. In this paper, we focus our investigation on the problem of inter-domain routing in MANETs. In the Internet, the Border Gateway Protocol (BGP) [8] provides a well-established mechanism for inter-domain routing among heterogeneous domains, called autonomous systems (AS). The principle of BGP is to enable *opaque* interoperation, where each domain has the administrative control over its intra-domain routing protocol and inter-domain routing policy, which is not known (or opaque) to the other domains.

Unlike in the Internet, the inter-domain routing problem is fundamentally different in MANETs with significant challenges. First, in MANETs, the network connectivity changes dynamically, thus an inter-domain routing protocol must be able to cope with such changes as network partitions/merges and connectivity changes. In addition, there are no clear boundaries between network domains and in many cases multiple domains may overlap in the same geographic region. Second, MANET environment has spawned out a new breed of routing protocols such as reactive routing protocols, geo-routing protocols, etc. [1] that are specialized for dynamic networks, and they require special handling to participate in inter-domain routing.

In this paper, we propose a novel networking framework, called IDRM (**I**nter-**D**omain **R**outing for **M**ANETs) to enable inter-domain routing between MANETs (and between MANETs and the Internet). IDRM has been designed to effectively address the two main challenges identified above. Particularly, it employs a proactive routing for inter-domain gateway communication to readily detect any topology changes (within a domain and among domains), and adapt to those changes. It supports each domain to participate in the

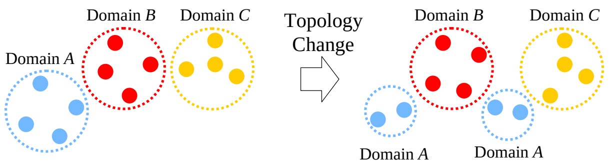

Figure 1: The MANET of domain A is partitioned due to mobility.

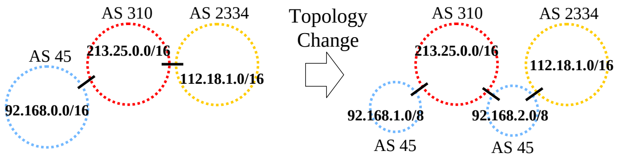

Figure 2: A similar setting in terms of topology change in BGP.

inter-domain routing operation without any changes to their native intra-domain routing protocols. It also supports a policy-based routing in the same spirit as in the Internet to allow business relations and administrative control could be specified. This will allow a seamless integration of IDRM with the BGP when MANETs need to interoperate with the wired network.

2. INSUFFICIENCY OF EXTANT ROUTING FRAMEWORKS

In this section, we discuss why extant routing frameworks are insufficient to support inter-domain routing in MANETs. Particularly, we explain why a BGP-like protocol is inapplicable in the ad hoc environment, and what in extant ad hoc routing frameworks are missing to support interoperation among multiple MANET domains.

2.1 Inadequacy of BGP for MANETs

Consider Figure 1, which consists of three MANET domains. One might apply a BGP-like protocol to this scenario as in Figure 2. However, there are several issues that render such a protocol inapplicable. First, the path vector protocol in BGP implicitly assumes the availability of the following functions:

(1) **Internal Gateway Detection:** The internal gateways within the same domain can detect the presence of each other so that they can communicate about the information of external routes.

(2) **Internal Network Knowledge:** The gateways know the reachable destinations and the internal routes to the destinations within the domain.

These functions are normally supported by the proactive intra-domain routing protocols through continual maintenance of network state information. However, we cannot always assume the availability of this information in MANETs that use a reactive routing protocol in their domains. Also a direct application of a path vector protocol over MANETs to support these functions may be undesirable to MANETs with dynamic node mobility and scarce wireless communication bandwidth.

Second, in BGP every destination is identified by an IP address, which follows a certain network hierarchy. To announce the destinations in a domain, gateways will aggregate the IP addresses in the domain by suitable IP prefixes (e.g., 92.168.0.0/16). However, in MANETs, mobility can create arbitrary network partition, unlike the perfect split of IP addresses as in Figure 2. Hence, IP prefixes do not suitably aggregate the IP addresses in partitioned MANETs and thus we cannot use the prefix-based routing of BGP.

Third, BGP relies on a path vector protocol that filters the paths consisting of repeated AS numbers to prevent looping. For example, in Figure 2, after topology change, the inter-domain level path from a source in AS 45 (92.168.1.0/8) to AS 2334 (112.18.0.0/16) is AS 45→AS 310→AS 45→AS 2334. This path will be filtered by the BGP path vector protocol, and hence it will prevent the nodes in AS 45 (92.168.1.0/8) from reaching AS 2334 (112.18.0.0/16).

In general, the design considerations for inter-domain routing in MANETs are fundamentally different from that of BGP. The main challenge of BGP is to cope with the extreme scale of the Internet; however, the scale of the network is not the main concern in MANETs since they will be relatively small due to physical/wireless, technical, and geographical constraints. Rather the main challenge here is to handle the constant changes in the network connectivity at both individual node level and at network domain level due to node mobility.

2.2 Insufficiency of current ad hoc protocols

In the literature, there are several proposals to enable interoperations among multiple wireless domains [5] [9]. Most of them only focus on high level architectures and provide a sketch of required components (e.g., translation of different naming spaces, and different protocols). While these related works have considered various issues regarding interoperation of multiple networks, none of them provided a specific solution for inter-domain routing between MANETs.

In the wireless context, there have been proposals to take advantage of heterogeneous routing protocols to adapt to network dynamics and traffic characteristics. For example, hybrid routing protocols (e.g. SHARP [7]) uses both proactive and reactive routing protocols to adapt the routing behavior according to traffic patterns. The basic idea is to create proactive routing zones around nodes where there are lots of data traffic, and use reactive routing in other areas. Since the main goal of hybrid routing is to improve the routing performance in a *single* domain via adaptation, it cannot support the interaction of multiple domains with different routing protocols.

Another related approach is cluster-based networking in MANETs [3]. The idea of cluster-based networking is to form self-organizing clusters and a routing backbone among cluster heads. In this way, cluster-based networks can use hierarchical routing and achieve a scalable routing solution in a single domain. Although cluster-based routing has a structural similarity to inter-domain routing, they are essentially addressing two fundamentally different problems. The goal of inter-domain routing is to support multiple domains with *autonomous* control; on the other hand, a cluster-based routing is applicable in a single domain with a full control over its clusters (e.g., on cluster formation and cluster head election, etc.).

3. DESIGN OF IDRM

In this section, we present the design of a networking framework called IDRM (Inter-Domain Routing for MANETs) to support opaque interoperations among multiple domains of MANETs. In this framework, each domain retains administrative control within its own domain while participating in collaboration. To enable inter-domain communications, IDRM requires special nodes as *gateways*. The role of gateways is more than just handling inter-domain routing; they need to bridge any technical seam that may exist between MANETs at physical, MAC, and network layers. However, the main focus of this paper is limited to the inter-domain routing functions of the gateways. A non-gateway node does not participate in the communication with the nodes in another domain. Thus multiple MANET domains may operate in the same region.

3.1 Design Issues

Now we explain the key design points of the IDRM. There are several issues that we need to handle: (1) partition and merge of domains, (2) membership announcement, (3) support for policy-based routing, and (4) data plane operations. The first two points are due to node mobility and dynamic topology, and the latter two are general issues with inter-domain routing with autonomy of each domain.

3.1.1 Handling Domain-level Topology Changes

As discussed in the previous section, one of the key challenges for inter-domain routing in MANET is dynamic changes of the network topology. In particular, a single domain may be partitioned into multiple MANETs due to node mobility and the gateways in the domain must detect the event. In a domain where the intra-domain routing protocol is proactive, this event will be eventually detected via route updates. For a domain with a reactive intra-domain routing protocol, however, this event may not be detected for a long time. To handle this problem, in IDRM, the gateways maintain soft state by periodically sending beacons to each other. The period of beacon can be adaptively set based on the mobility of the nodes and the rate of topology change.

After detecting a partition, the gateways in the same partition should generate a new MANET ID so that the new partition can be uniquely identified. By dynamically assigning a new ID, we can prevent the path vector routing algorithm from mistakenly considering the route via partitioned networks as a loop.[1] This computation should be performed independently at each gateway in the way that (1) all the gateways in the same partition to generate the same ID, and (2) the collision of IDs of different networks to be as low as possible. One way to achieve these goals is to use a pseudo random number generator to create a new ID using the IDs of all the gateways in the network as input. The gateways in the same partition use a simple hash function (e.g., MD5) to generate a random number, then prefix it by the domain ID to get a new MANET ID. We encode the domain ID in the new MANET to support a dynamic policy translation (as discussed in 3.1.3 and [11]). Conversely, when multiple partitioned MANETs come close and get re-connected, this condition should be detected by the gateways and a new ID for the merged MANET should be generated. This follows the same process as the case of network partitioning.

3.1.2 Membership Management and Announcement

Periodically gateways should advertise the IDs of the nodes that they can reach; for this the gateways need to collect the IDs of all the nodes in the MANET for advertisement of the membership to other domains. As we pointed out earlier, in MANETs we cannot rely on IP prefix for routing between domains due to arbitrary partitions and merges. There are two possible approaches to deal with the situation. First, the gateways can coordinate and reassign the node IDs so that each MANETs can have a unique prefix every time a topology change occurs. However, this will incur significant management overhead (e.g., to generate unique prefix, generate unique node IDs, to update name-to-ID mapping) and thus will only be useful when the new topology will remain unchanged for a relatively long time.

Second, a more practical approach to handle topology changes is to let the gateways in partitioned networks advertise the membership information, and this membership digest is used for inter-domain routing. For a reasonable size MANET with less than 1000 nodes, we find that a plain membership digest containing a set of node IDs (e.g., IP addresses) without any compression is better than a more scalable solution [12]. Obviously, the second approach (based on membership digest) can cope with network dynamics better and is more graceful when partitioned MANETs merge (by just merging the memberships). Hence, we employ the second approach in IDRM.

Keeping track of the non-gateway membership in a domain poses a similar challenge to network partition detection; in a reactive routing domain, a gateway may have a stale view of its membership, and can only discover the membership change when it has data to transfer. Although we can periodically perform a membership query, this can be potentially expensive. Thus instead, we let a reactive domain only initiate a membership query when there is an indication that its membership may have changed, e.g., a node in the membership digest cannot be reached, *and* a timeout period has passed.

3.1.3 Policy Support

Inter-domain routing policy is enforced in a similar same way as in BGP. By exchanging route updates (announcements and withdrawal) in a path vector protocol, inter-domain routing policies will be translated as the decisions of filtering and selecting routes at gateways. Using a path vector protocol, if a gateway a_1 in domain A is willing to provide a transit service to a neighboring domain B for a destination c_1, then a_1 appends its MANET ID to the route announcement of the selected path to c_1 and announces it to a connected gateway b_1 in domain B. Upon receiving the announcement, b_1 will decide if this path is more preferable than the current using path to c_1 based on its routing policy. If a new path is selected, b_1 will record the source of announcement as a_1 and distributes the announcement to other internal gateways in the MANET.

There are a variety of ways to specify routing policy rules. For example, in a next-hop-based policy specification, gateways will select paths only based on the next-hop domain in the route announcement (based on commercial relations like

[1] It is possible to extend this basic protocol to include a leader election process and let the leader of a domain coordinate intra-domain operations (e.g., hierarchical beaconing among gateways, or MANET ID generation). But we do not discuss such schemes here for simplicity.

customer, provider, or peer). In a path-based specification, a domain will specify a complete ordered preference of all the acyclic domain-level paths; paths with higher rank are more preferable. In a cost-based specification, a domain will assign a numerical cost to every other domain as a subjective evaluation of the performance. Gateways will select the paths with the minimum total cost of all the downstream domains. In our design, we do not restrict the way inter-domain policies could be specified, but we assume that a next hop specification is used in our description.

One important issue to address in MANETs is that these routing policies are defined by network operators as static rules. Now in a MANET environment, a single domain may partition into multiple networks (e.g., a domain A breaks down into A_1 and A_2). Thus it is necessary to have a mechanism to automatically translate the original policy when such topology change happens. In [11], we have reported preliminary results on how to translate the static policies when a domain partitions under the next-hop-based specification and the cost-based specification. We refer the reader to [11] for more discussion on this topic. In general, designing a mechanism to handle dynamic policy translation for MANETs is an interesting topic requiring further research.

3.1.4 Data Plane Operations

When a node sends data packets to an external destination (in another domain or in another partitioned network), it forwards the packets to one of the reachable intra-domain gateways. In a reactive domain, the sending node will first initiate a route discovery, and a gateway node that has a route to the destination will respond. In a proactive domain, the sending node will have a list of intra-domain gateways, and select one of them based on its own preferences. In either case, the gateway will first see if it is directly connected to the domain that contains the destination. If it is then it just forwards the packet; otherwise, it will forward the packets to a gateway connected to the destination domain based on the inter-domain routing information.

For incoming packets, the gateway performs a protocol translation and invokes the intra-domain routing protocol. In a reactive domain, the gateway will initiate a route discovery process if it does not already have the route in the cache. In a proactive domain, the gateway can determine if the destination is reachable from the local routing table.

If for some reasons the destination cannot be reached (e.g., the node may have been disconnected from any domain) IDRM does not provide feedback for unreachable destination. Following the design principles of the Internet, the problem should be handled at a higher layer. Although we only discuss proactive and reactive routing protocols in this paper, it is not difficult to see that this framework can support other types of intra-domain routing protocols (e.g., georouting and hybrid routing). Thus we do not present these cases in this paper.

3.2 Protocol Specification

This section describes the inter-domain routing protocol of IDRM in pseudo codes. We present three algorithms to be executed at each gateway. Algorithm 1 is a subroutine to generate route updates (including route announcement and withdrawal). Algorithm 2 is a continual process of a gateway to handle the interaction between inter-domain gateways. Algorithm 3 is a continual process to manage the intra-domain membership.

For a gateway i in a domain A, let $G^{\mathsf{intra}}(i)$ denote a set consisting of the intra-domain gateways to that i has connectivity, and $G^{\mathsf{inter}}(i)$ denote a set consisting of the inter-domain gateways i is directly connected. Let $M(i)$ denote the set of intra-domain members to that i has connectivity.

Algorithm 1 Route Announcement Update

```
need_update ← FALSE
if ([MD, path] $\neq$ NULL) then
  withdraw[MD, path] ← [MD, path]
end if
// store old route annoucement for withdrawal
if (any change in $G^{\mathsf{intra}}(i)$) then
  // generate a new MANET_ID
  MANET_ID ← $f(A, G^{\mathsf{intra}}(i))$
  need_update ← TRUE
  // else MANET_ID does not change
end if
if (any change in $M(i)$) then
  // generate a new membership digest
  MD ← $b(M(i))$
  need_update ← TRUE
  // else the membership digest does not change
end if
path ← {MANET_ID}
return a new route announcement [MD, path]
```

Algorithm 1 checks any change in the membership of $G^{\mathsf{intra}}(i)$ and $M(i)$, and generate a new route announcement if necessary, and a route withdrawal that uses old membership information and MANET ID. Here, the function f denotes a one-way hash function (e.g., MD5) to create a MANET_ID based on the original domain ID, and the set of gateways, and the membership digest based on $M(i)$ (see Section 3.1.2 for how to obtain $M(i)$).

Algorithm 2 Main Routine of the Gateway

```
while (true) do
  if (timer > announcement interval) then
    // generate a new route announcement
    call Algorithm 1
    if need_update then
      send route withdrawal withdraw[MD, path] to $G^{\mathsf{inter}}(i)$
      send route announcement [MD, path] to $G^{\mathsf{inter}}(i)$
    end if
  end if
  // propagate route withdrawal
  if (received a route withdrawal withdraw[MD, path]) then
    // update the path vector
    delete [MD, path]
    path ← append (MANET_ID, path)
    announce withdraw[MD, path] to $G^{\mathsf{inter}}(i) \cup G^{\mathsf{intra}}(i)$
  end if
  // propagate route announcement
  if (received a route announcement [MD, path]) then
    if (announcement from $g^{\mathsf{new}}$ not in $G^{\mathsf{inter}}(i)$) then
      // new connected inter-domain gateway found
      $G^{\mathsf{inter}}(i) \leftarrow G^{\mathsf{inter}}(i) \cup \{g^{\mathsf{new}}\}$
    end if
    if ((no route to MD) OR (path $\prec$ route to MD)) then
      // update the path vector
      insert [MD, path] at the top
      path ← append (MANET_ID, path)
      announce [MD, path] to $G^{\mathsf{inter}}(i) \cup G^{\mathsf{intra}}(i)$
    end if
  end if
  increment timer and sleep
end while
```

Algorithm 2 presents the main function of a gateway participating in IDRM. The main routine consists of two parts. First, it periodically polls its domain status, generates a new route announcement or route withdrawal, and broadcasts the route updates to its neighbouring inter-domain gateways. Second, it wakes up when a new route withdrawal or announcement is received from one of its neighbours and process them. In the route announcement, **path** is an ordered list of MANET_IDs, i.e., [MANET_ID$_1$, …, MANET_ID$_n$], which indicates the nodes in MD can be reached by traversing MANET_ID$_1$, then MANET_ID$_2$, …, and finally MANET_ID$_n$. When it processes a route withdrawal, it first deletes the path vector as indicated by route withdrawal, and then propagate the route withdrawal by appending its MANET ID. When it processes a route announcement, it first examines if the origin of the announcement is already in its list of neighbours. If it is a new neighbour it updates the list. Then it compares the new path information using its inter-domain routing policy. If the route specified in the **path** is allowed and is more preferable than the current route to MD based on inter-domain routing policy (i.e., **path** $\prec$ route to MD), the gateway updates its routing table by inserting the new route to the top (assuming that the preference of a route is determined by the order in the routing table), and then appends its own MANET ID in front of **path** and rebroadcasts the information to its neighbours.

Algorithm 3 Beaconing among Intra-domain Gateways

```
while (true) do
  if (timer > beacon interval) then
    send beacons to every gateway in $G^{\mathsf{intra}}(i)$
  end if
  for all (gateway $g$ in $G^{\mathsf{intra}}(i)$) do
    if (no beacons from $g$ within time limit) then
      // network has partitioned
      $G^{\mathsf{intra}}(i) \leftarrow G^{\mathsf{intra}}(i) \backslash \{g\}$
      raise change flag
    end if
  end for
  if (received a beacon from $g$ not in $G^{\mathsf{intra}}(i)$) then
    // network merge event OR new gateway
    $G^{\mathsf{intra}}(i) \leftarrow G^{\mathsf{intra}}(i) \cup \{g\}$
    raise change flag
  end if
  if (change flag is up) then
    // generate a new route announcement
    call Algorithm 1
    send the route announcement to $G^{\mathsf{inter}}(i)$
    reset change flag
  end if
  increment timer and sleep
end while
```

Algorithm 3 is a separate thread that takes care of the exchange of beacons among the gateways in the same domain. Periodically, a gateway sends out a beacon to all intra-domain gateways notifying its presence. When it does not receive a beacon from one or more of the gateways in its intra-domain, it updates $G^{\mathsf{intra}}(i)$. Similarly, when it receives a beacon from a gateway g that is not currently in the list of intra-domain gateways, it updates its entry. When these changes are detected, the gateway initiates a route announcement process to update its neighbours.

4. OVERHEAD ANALYSIS

In this section, we study the feasibility of the proposed IDRM protocol by estimating the message overhead incurred by the protocol. Our analysis aims to convey a basic picture of the estimated overhead, without involving the detailed steps of the protocol. We assume that no control packets are dropped or retransmitted, and the inter-domain routing policies are simple, so that gateways will not switch forwarding paths except when the paths are disconnected. Our analysis follows a similar approach for analyzing proactive and reactive routing protocols in [4].

Symbol	Defintion
N	Total number of nodes in a domain
G	The number of gateways in a domain
r	Transmission radius
$\bar{\nu}$	Average speed of a node
$\bar{E}$	Average number of links in a domain

Table 1: Definitions of parameters

First, consider a single domain with the parameters as defined in Table 1. Assume that the mobility process of nodes is stationary and be confined to a bounded area. For a pair of nodes, if one node moves out of the transmission radius of other, then the link between them breaks. So, the average lifespan of a link is $\Theta\big(r/\bar{\nu}\big)$, and the average number of link breakages per second due to mobility is $\Theta\big(\bar{E}\bar{\nu}/r\big)$.

Since the mobility process of nodes is stationary where there is no net links are created or broken over time, the average numbers of link creations per second due to mobility in the domain is also $\Theta\big(\bar{E}\bar{\nu}/r\big)$. Hence, the average number of link state changes (creations or breakages) per second is $\Theta\big(\bar{E}\bar{\nu}/r\big)$. The control overhead of intra-domain routing protocols is determined by the number of link state changes.

Next, we estimate the overhead for proactive intra-domain routing protocols, reactive intra-domain routing protocols, and inter-domain routing protocol, respectively.

(1) **Proactive Intra-domain Routing Protocols:** Each node periodically broadcasts hello packets to its neighbours. Based on the received hello packets, each node announces a new link-state/distance-vector packet that will be propagated throughout the MANET. Let λ^{hel} be the number of hello packets broadcast by each node per second. The total number of hello packets per second is $\lambda^{\mathsf{hel}}N$.

Since the average number of link state changes per second is $\Theta\big(\bar{E}\bar{\nu}/r\big)$, the total number of link-state/distance-vector packets per second broadcast is $\mathrm{O}\big(\bar{E}^2\bar{\nu}/r\big)$. This is an upper bound because optimized broadcast-based protocols (e.g., OLSR) normally requires less than $\bar{E}$ transmissions for each link-state/distance-vector packet to propagate throughout the network. Thus, the estimated number of control packets per second is:

$$\lambda^{\mathsf{hel}}N + \mathrm{O}\big(\bar{E}^2\bar{\nu}/r\big) \tag{1}$$

This is also the control overhead per second (at domain level) by IDRM to detect network partition and merging.

(2) **Reactive Intra-domain Routing Protocols:** IDRM requires beaconing among gateways to detect network partition or merging. The number of gateway pairs that will beacon each other is upper bounded by $\mathrm{O}(G^2)$. Let λ^{bea} be the beaconing rate between a pair of gateways. Then total number of beacons per second by gateways is $\mathrm{O}(\lambda^{\mathsf{bea}}G^2)$.

Let $\bar{L}$ be the average number of hops between a pair of nodes in the MANET. The number of link state changes per second for a path between a pair of gateways is: $\Theta\big(\bar{L}\bar{\nu}/r\big)$. Since each link state change will incur maintenance overhead in reactive routing protocols, it is reasonable to assume that the number of control packets is proportional to the number of link state changes and the beaconing traffic. Hence, the estimated number of control packets per second required by IDRM to detect network partition and merging is:

$$\mathrm{O}\Big(\lambda^{\mathsf{bea}} G^2 \bar{L}\bar{\nu}/r\Big) \tag{2}$$

(3) **Inter-domain Routing Protocol:** Suppose there are m^{pro} domains running proactive routing protocols and m^{rea} domains running reactive routing protocols. Also assume each domain has the same parameters as in Table 1. Note that the path vector protocol in IDRM behaves like a proactive routing protocols, but with different parameters. Let λ^{inter} be the number of inter-domain hello packets broadcast by each gateway per second in the path vector protocol. The total number of hello packets generated in the multi-domain MANET per second is $(m^{\mathsf{pro}}+m^{\mathsf{rea}})\lambda^{\mathsf{inter}}\bar{G}$, where $\bar{G}$ denotes the average number of gateways in each domain.

If a pair of intra-domain gateways stay in the same MANET, there may be multiple paths connecting them. Let $1/\mu$ be the average lifespan of the connectivity between a pair of intra-domain gateways. That is, μ is the connectivity breakage rate of connected pairs of intra-domain gateways due to mobility. By stationarity of mobility process, μ is also the rate of change for the connectivity status of intra-domain gateways. Since IDRM will carry out new membership management and announcement when the connectivity status between a pair of intra-domain gateways is changed, the estimated number of connectivity status changes is:

$$\mathrm{O}\Big((m^{\mathsf{pro}}+m^{\mathsf{rea}})\mu\bar{G}^2\Big)$$

Hence, the total number of control packets per second for path vector protocol is:

$$(m^{\mathsf{pro}}+m^{\mathsf{rea}})\lambda^{\mathsf{inter}}\bar{G} + \mathrm{O}\Big((m^{\mathsf{pro}}+m^{\mathsf{rea}})\mu\bar{G}^2\bar{E}^{\mathsf{inter}}\Big) \tag{3}$$

where $\bar{E}^{\mathsf{inter}}$ is the average number of pairs of connected inter-domain gateways in the $(m^{\mathsf{pro}}+m^{\mathsf{rea}})$ domains.

In a given network, $m^{\mathsf{pro}}, m^{\mathsf{rea}}, \bar{G}, \bar{E}$, and λ^{inter} are fixed. It is not straightforward to decide μ. But we can obtain this value from simulation. In Figure 3, we observe μ decreases as the number of nodes increases because as a MANET becomes denser, the connectivity between a pair of gateways becomes more stable, whereas node speed adversely affects the stability of links almost linearly.

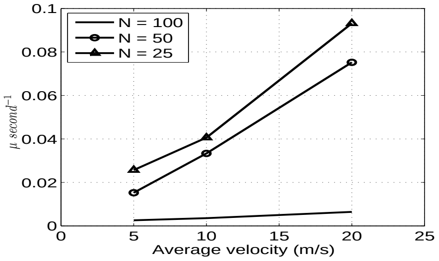

Figure 3: Average lifespan of the connectivity between a pair of intra-domain gateways.

Note that Eq. (3) only provides an asymptotic result for the *total* control overhead incurred by IDRM without any optimization. Since the overhead will be distributed among all the gateways and various optimization can be applied (e.g., suppression of hello, adaptive adjustment of probing interval), the overhead incurred at each gateway for inter-domain routing operation will be quite moderate.

We compare this estimation to the normal routing overhead (not incurred by inter-domain routing). The overhead for proactive domains is Eq. (1), and the same for reactive domains is Eq. (2). Note that N and $\bar{E}$ are typically orders of magnitude greater than the other parameters. Thus, the overhead from reactive domains and inter-domain operations are substantially small compared to proactive domains.

To summarize, in a multi-domain MANET consisting of proactive and reactive domains, the overall control overhead is dominated by that of the proactive domains, and the overhead incurred by inter-domain routing protocol is relatively insignificant. Thus we report that inter-domain routing can be supported with moderate additional overheads in MANETs, and IDRM is a viable approach to enable that.

5. CONCLUSION

Inter-domain routing offers a means for heterogeneous MANETs to interoperate with each other. This paper has identified the challenges of inter-domain routing in MANETs, and proposed IDRM as a viable solution. This paper has shown that, despite dynamic network topology and diverse intra-domain ad hoc routing protocols, opaque interoperation among heterogeneous multi-domain MANETs can be supported. We also discussed how IDRM can support network operators to specify inter-domain routing policies in a similar manner as BGP. This is an important feature to encourage interoperation among multiple MANET domains in practice. We expect that IDRM will improve the end-to-end reachability of mobile users, and consequently enhance the usefulness of MANETs.

6. REFERENCES

[1] M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, 2:1–22, 2004.

[2] A. Broder and M. Mitzenmacher. Network applications of bloom filters: A survey. *Internet Mathematics*, 1(4):485–509.

[3] Y. Chen, A. Liestman, J. Liu. Clustering algorithms for ad hoc wireless networks. In *Proc. Ad Hoc and Sensor Networks '04*.

[4] T. Clausen, P. Jacquet, and L. Viennot. Analyzing control traffic overhead versus mobility and data traffic activity in mobile ad-hoc network protocols. *ACM Wireless Networks journal (Winet)*, 10(4), July 2004.

[5] J. Crowcroft et. al.. Plutarch: an argument for network pluralism. *ACM Computer Communication Review*, 33(4):258–266, 2003.

[6] Y.-C. Hu, A. Perrig, and M. Sirbu. SPV: Secure path vector routing for securing BGP. In *Proc. ACM SIGCOMM*, 2004.

[7] V. Ramasubramanian, Z. J. Haas, and E. G. Sirer. SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks. In *Proc. ACM MOBIHOC*, June 2003.

[8] Y. Rekhter and T. Li. RFC 1771: a Border Gateway Protocol 4 (BGP-4), March 1995.

[9] S. Schmid, L. Eggert, M. Brunner, and J. Quittek. TurfNet: An architecture for dynamically composable networks. In *Proc. of WAC 2004*, October 2004.

[10] W. Ma, M. Chuah. Comparisons of inter-domain routing schemes for heterogeneous ad hoc networks. In *Proc. of WOWMOM '05*.

[11] C.-K. Chau, J. Crowcroft, K.-W. Lee, S. H.Y. Wong, How to Enable Policy-based Interactions in Dynamic Wireless Networks? In *IEEE Workshop on Policies, 2008*.

[12] C.-K. Chau, J. Crowcroft, K.-W. Lee, S. H.Y. Wong, IDRM: Inter-domain Routing Protocol for Mobile Ad Hoc Networks. Computer Lab, University of Cambridge. Technical Report UCAM-CL-TR-708, 2007, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-708.html.